UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/401,596	09/22/1999	DAVID M CHESS	909.0001USU	4869

7590 03/23/2004

HARRY F SMSITH ESQUIRE
OHLANDT GREELEY RUGGIERO & PERLE LLP
ONE LANDMARK SQUARE
SUITE 903
STAMFORD, CT 06901

EXAMINER	
ABEL JALIL, NEVEEN	
ART UNIT	**PAPER NUMBER**
2175	

DATE MAILED: 03/23/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/401,596	CHESS, DAVID M	
	Examiner	Art Unit	
	Neveen Abel-Jalil	2175	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 September 1999*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-37* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1, 3-15, 17-29,31-33, and 35-37* is/are rejected.

7)☒ Claim(s) *2,16,30 and 34* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date 2.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Specification

1. The abstract of the disclosure is objected to because in the abstract, line 1, "is disclosed" should be deleted. Correction is required. See MPEP § 608.01(b).

Applicant is reminded of the proper language and format for an abstract of the disclosure.

The abstract should be in narrative form and generally limited to a single paragraph on a separate sheet within the range of 50 to 150 words. It is important that the abstract not exceed 150 words in length since the space provided for the abstract on the computer tape used by the printer is limited. The form and legal phraseology often used in patent claims, such as "means" and "said," should be avoided. The abstract should describe the disclosure sufficiently to assist readers in deciding whether there is a need for consulting the full patent text for details.

The language should be clear and concise and should not repeat information given in the title. It should avoid using phrases which can be implied, such as, "The disclosure concerns," "The disclosure defined by this invention," "The disclosure describes," etc.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1, 3-15, 17-29, 31-33, and 35-37 rejected under 35 U.S.C. 103(a) as being unpatentable over Chen et al. (U.S. Patent No. 5,960,170) in view of Dotan (U.S. Patent No. 5,822,517).

As to claim 1, Chen et al. discloses a virus detection method for use in a computer system comprising at least one object that may potentially become infected with a computer virus, comprising steps of:

for an object that is indicated as having a current state that is described by the stored information, programmatically examining the object for a presence of a computer virus while assuming that the current state of the object is the same as the state of the object as it existed at the point in the past (See column 9, lines 11-62, also see column 12, lines 12-67).

Chen et al. does not teach providing a database comprised of stored information that is descriptive of a state of the at least one object as it existed at a point in the past.

Dotan teaches providing a database comprised of stored information that is descriptive of a state of the at least one object as it existed at a point in the past (See Dotan column 11, lines 28-48).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time of the invention was made to have modified Chen et al. to include providing a database comprised of stored information that is descriptive of a state of the at least one object as it existed at a point in the past.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have modified Chen et al. by the teaching of Dotan to include providing a database comprised of stored information that is descriptive of a state of the at least one object as it existed at a point in the past because storing the state of the object will allow for accurate comparison for virus detection and prevention.

As to claim 3, Chen et al. as modified discloses wherein the stored information is descriptive at least in part of a number and location of archived objects within the object (See figure 4C, shows locations storing object by "Virus Identifier").

As to claim 4, Chen et al. as modified discloses wherein the stored information is descriptive at least in part of features of the object that serve as inputs to a neural network-based virus detection system, and wherein the step of programmatically examining the object comprises a step of operating the neural network-based virus detection system using the features as inputs (See column 19, lines 1-38).

As to claim 5, Chen et al. as modified discloses wherein the stored information is descriptive at least in part of whether at least one macro is present within the object (See column 19, lines 1-38).

As to claim 6, Chen et al. as modified discloses wherein the stored information is descriptive at least in part of whether at least one archived object is present within the object (See figure 4C, shows locations storing object by "Virus Identifier").

As to claim 7, Chen et al. as modified discloses wherein the stored information is descriptive at least in part of whether the object can possibly be infected with a virus according to predetermined criteria, and wherein the step of programmatically examining is executed only if the stored information indicates that the object may possibly be infected according to the

predetermined criteria as compared to criteria that are currently in effect (See column 12, lines 1-67).

As to claim 8, Chen et al. as modified discloses wherein if it is indicated that a current state of the object is not described by the stored information, the step of programmatically examining comprises an initial step of processing the object to ascertain the current state of the object, and storing information in the database that is descriptive of the current state of the object (See Dotan column 4, lines 21-64).

As to claim 9, Chen et al. as modified discloses wherein the stored information comprises, for an object that contains in archived or combined form at least one other object, information descriptive of whether the at least one contained object is of a type that should be examined for computer viruses, and wherein the step of programmatically examining avoids re-determining and re-scanning the contained at least one object if the stored information indicates that the at least one contained object is not required to be scanned (See column 3, lines 8-64).

As to claim 10, Chen et al. as modified discloses wherein the stored information comprises, for an object that contains in archived or combined form at least one other object, information descriptive of at least one of a location, extent, or encoding -method of the at least one contained object, and wherein the step of programmatically examining is responsive to the stored information for reducing an amount of processing time required to extract the at least one

contained object in order to examine the at least one contained object (See column 27, lines 5-35).

As to claim 11, Chen et al. as modified discloses wherein the stored information comprises information descriptive of a location of an entry-point of the object, and wherein the step of programmatically examining uses the stored information to determine the entry-point of the object, if the database indicates that the object has not changed since the entry point information was stored (See column 11, lines 52-67, and see column 12, lines 1-67).

As to claim 12, Chen et al. as modified discloses wherein the stored information comprises information descriptive of a structure of the object, and wherein the step of programmatically examining uses the stored information to determine the structure of the object, if the database indicates that the object has not changed since the structure information was stored (See Dotan column 7, lines 11-51, also see Chen et al. column 3, lines 28-67).

As to claim 13, Chen et al. as modified discloses wherein the stored information comprises information descriptive of at least one of a number, size, name, extent, or other attribute of macros or other units of active content in the object, and wherein the step of programmatically examining uses the stored information to determine at least one of the number, size, name, extent, or other attribute of macros or other units of active content in the object, if the database indicates that the object has not changed since the information was stored (See column 18, lines 1-16, also see column 11, lines 22-51, and see column 14, lines 32-67).

As to claim 14, Chen et al. as modified discloses wherein the step of programmatically examining includes a program- emulation step for executing the current object in a virtual environment, for collecting data resulting from the execution in the virtual environment, and for storing at least some of the results produced by the program- emulation step in the database, and wherein the step of programmatically examining uses the stored results rather than re-executing the program-emulation step, if the database indicates that the object has not changed since the results were stored (See Dotan column 8, lines 18-67, and see Chen et al. column 3, lines 28-67).

As to claim 15, Chen et al. discloses virus detection component for use in a computer system that stores at least one object that may potentially become infected with a computer virus, comprising:

an object examination unit bi-directionally coupled to said database and responsive to a determination that an object has a current state that is described by the stored information, for programmatically examining the object for a presence of a computer virus while using the stored information from said database (See column 9, lines 11-62, also see column 12, lines 12-67).

Chen et al. does not teach providing a database comprised of stored information that is descriptive of a state of the at least one object as it existed at a point in the past.

Dotan teaches providing a database comprised of stored information that is descriptive of a state of the at least one object as it existed at a point in the past (See Dotan column 11, lines 28-48).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time of the invention was made to have modified Chen et al. to include providing a database comprised of stored information that is descriptive of a state of the at least one object as it existed at a point in the past.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have modified Chen et al. by the teaching of Dotan to include providing a database comprised of stored information that is descriptive of a state of the at least one object as it existed at a point in the past because storing the state of the object will allow for accurate comparison for virus detection and prevention.

As to claim 17, Chen et al. as modified discloses wherein the stored information is descriptive at least in part of a number and location of archived objects within the object (See figure 4C, shows locations storing object by "Virus Identifier").

As to claim 18, Chen et al. as modified discloses wherein the stored information is descriptive at least in part of features of the object that serve as inputs to a neural network-based virus detection system, and wherein said neural network-based virus detection system uses the features as inputs (See column 19, lines 1-38, also see column 21, lines 3-39).

As to claim 19, Chen et al. as modified discloses wherein the stored information is descriptive at least in part of whether at least one macro is present within the object (See column 19, lines 1-38).

As to claim 20, Chen et al. as modified discloses wherein the stored information is descriptive at least in part of whether at least one archived object is present within the object (See column 19, lines 1-29).

As to claim 21, Chen et al. as modified discloses wherein the stored information is descriptive at least in part of whether the object can possibly be infected with a virus according to predetermined criteria, and wherein said object examination unit programmatically examines said object only if the stored information indicates that the object may possibly be infected according to the predetermined criteria as compared to criteria that are currently in effect (See column 12, lines 1-67).

As to claim 22, Chen et al. as modified discloses wherein if said determination indicates that a current state of the object is not described by the information stored in said database, said object examination unit first processes the object to ascertain the current state of the object, and stores information in said database that is descriptive of the current state of the object (See Dotan column 4, lines 21-64).

As to claim 23, Chen et al. as modified discloses wherein the stored information comprises, for an object that contains in archived or combined form at least one other object, information descriptive of whether the at least one contained object is of a type that should be examined for computer viruses, and wherein said object examination unit inhibits re-determining

and re-scanning the contained at least one object if the stored information indicates that the at least one contained object is not required to be scanned (See column 19, lines 39-67, and see column 20, lines 1-24).

As to claim 24, Chen et al. as modified discloses wherein the stored information comprises, for an object that contains in archived or combined form at least one other object, information descriptive of at least one of a location, extent, or encoding-method of the at least one contained object, and wherein said object examination unit is responsive to the stored information for reducing an amount of processing time required to extract the at least one contained object in order to examine the at least one contained object (See column 18, lines 1-16, also see column 11, lines 22-51, and see column 14, lines 32-67).

As to claim 25, Chen et al. as modified discloses wherein the stored information comprises information descriptive of a location of an entry-point of the object, and wherein said object examination unit is responsive to the stored information to determine the entry-point of the object, if the database indicates that the object has not changed since the entry-point information was stored (See column 11, lines 52-67, and see column 12, lines 1-67).

As to claim 26, Chen et al. as modified discloses wherein the stored information comprises information descriptive of a structure of the object, and wherein said object examination unit is responsive to the stored information for determining the structure of the

object, if the database indicates that the object has not changed since the structure information was stored (See Dotan column 7, lines 11-51, also see Chen et al. column 3, lines 28-67).

As to claim 27, Chen et al. as modified discloses wherein the stored information comprises information descriptive of at least one of a number, size, name, extent, or other attribute of macros or other units of active content in the object, and wherein said object examination unit is responsive to the stored information for determining at least one of the number, size, name, extent, or other attribute of macros or other units of active content in the object, if the database indicates that the object has not changed since the information was stored (See column 18, lines 1-16, also see column 11, lines 22-51, and see column 14, lines 32-67).

As to claim 28, Chen et al. as modified discloses further comprising a program-emulation unit for executing the current object in a virtual environment, for collecting data resulting from the execution in the virtual environment, and for storing at least some of the results produced by the program-emulation unit in said database, and wherein said object examination unit is responsive to the stored results for using said stored results, and for inhibiting the operation of said program emulation unit, if the database indicates that the object has not changed since the results were stored (See Dotan column 8, lines 13-50, also see Chen et al. column .

As to claim 29, Chen et al. discloses a computer program embodied on a computer readable medium for providing a virus detection program subsystem, comprising:

an object examination code segment that is responsive to a determination that the object has a current state that is described by the stored information in said database, for programmatically examining the object for a presence of a computer virus while using the stored information from said database (See column 9, lines 11-62, also see column 12, lines 12-67).

Chen et al. does not teach a code segment for at least maintaining a database that stores information that is descriptive of a state of at least one object as the object existed at a point in the past.

Dotan teaches providing a code segment for at least maintaining a database that stores information that is descriptive of a state of at least one object as the object existed at a point in the past (See Dotan column 11, lines 28-48).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time of the invention was made to have modified Chen et al. to include a code segment for at least maintaining a database that stores information that is descriptive of a state of at least one object as the object existed at a point in the past.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have modified Chen et al. by the teaching of Dotan to include a code segment for at least maintaining a database that stores information that is descriptive of a state of at least one object as the object existed at a point in the past because storing the state of the object will allow for accurate comparison for virus detection and prevention.

As to claim 31, Chen et al. as modified discloses wherein said computer readable medium further stores a neural network based virus detection code segment, wherein said database further

stores information descriptive of features of the object that serve as inputs to said neural network-based virus detection code segment, and wherein said neural network-based virus detection code segment uses the features as inputs (See column 19, lines 1-38).

As to claim 32, Chen et al. as modified discloses wherein said computer readable medium further stores a program-emulation code segment for executing objects in a virtual environment, for collecting data resulting from the execution in the virtual environment, and for storing at least some of the results in said database, and wherein said object examination unit code segment is responsive to the stored results for using said stored results, and for inhibiting the operation of said program emulation unit code segment, if said database indicates that the object has not changed since the results were stored (See Dotan column 8, lines 18-67, and see Chen et al. column 3, lines 28-67).

As to claim 33, Chen et al. discloses a computer program embodied on a computer readable medium, the computer program being capable of executing a method for use in a computer system that comprises at least one object that may potentially become infected with a computer virus (See abstract), the method executed by the computer program comprising steps of:

for an object that the database indicates has a current state that is described by the stored information, programmatically examining the object for a presence of a computer virus while assuming that the current state of the object is the same as the state of the object as it existed at the point in the past (See column 9, lines 11-62, also see column 12, lines 12-67).

Chen et al. does not teach maintaining a database that is comprised of stored information that is descriptive of a state of the at least one object as it existed at a point in the past.

Dotan teaches maintaining a database that is comprised of stored information that is descriptive of a state of the at least one object as it existed at a point in the past (See Dotan column 11, lines 28-48).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time of the invention was made to have modified Chen et al. to include maintaining a database that is comprised of stored information that is descriptive of a state of the at least one object as it existed at a point in the past.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have modified Chen et al. by the teaching of Dotan to include maintaining a database that is comprised of stored information that is descriptive of a state of the at least one object as it existed at a point in the past because storing the state of the object will allow for accurate comparison for virus detection and prevention.

As to claim 35, Chen et al. as modified discloses wherein the stored information is descriptive at least in part of a number and location of archived objects within the object (See figure 4C, shows locations storing object by "Virus Identifier").

As to claim 36, Chen et al. as modified discloses wherein the computer program implements or has access to a neural network-based virus detection system, wherein the stored information is descriptive at least in part of features of the object that serve as inputs to the

neural network-based virus detection system, and wherein the step of programmatically examining the object comprises a step of operating the neural network-based virus detection system using the features as inputs (See column 19, lines 1-38).

As to claim 37, Chen et al. as modified discloses wherein for an object that the database indicates has a current state that is not described by the stored information, the step of programmatically examining comprises an initial step of operating the stored program to process the object to ascertain the current state of the object, and storing information in the database that is descriptive of the current state of the object (See Dotan column 4, lines 21-64).

Allowable Subject Matter

4. Claims 2, 16, 30, and 34 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

The prior art of record (Chen et al. -U.S. Patent No. 5,960,170, and Dotan -U.S. Patent No. 5,822,517) do not disclose, teach, or suggest the claimed limitations of (in combination with all other features in the claim), wherein the stored information is descriptive at least in part of a number and location of macros within the object, as found in claims 2, 16, and 34.

The prior art of record (Chen et al. -U.S. Patent No. 5,960,170, and Dotan -U.S. Patent No. 5,822,517) do not disclose, teach, or suggest the claimed limitations of (in combination with

all other features in the claim), computer readable medium further stores a list comprised of information that is descriptive of at least one of known viruses and of known classes of viruses, said list being used by said object examination code segment when programmatically examining the object for the presence of a computer virus, as found in claim 30.

Conclusion

5. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Neveen Abel-Jalil whose telephone number is 703-305-8114. The examiner can normally be reached on 8:00AM-4: 30PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Dov Popovici can be reached on 703-305-3830. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Charles Rones

CHARLES RONES
PRIMARY EXAMINER

Neveen Abel-Jalil
March 10, 2004